Abstract of the Disclosure

A two-tier security architecture that provides balance between the use of public and secret-key cryptography to realize cost-effectiveness and scalability of security. One tier is an intra-zone tier and the other tier is an inter-zone tier. The intra-zone tier addresses communication between users employing endpoints within a prescribed Security Zone and is designed to achieve cost-effectiveness. The inter-zone tier specifies how communication between users employing endpoints from different Security Zones can be established and is designed to provide scalability for intra-enterprise and/or inter-enterprise communications. Specifically, each Security Zone has a "Zone Keeper" and one or more endpoints that may be employed by users. The Zone Keeper authenticates, i.e., validates, users employing an endpoint in the Security Zone and determines whether a caller and a callee are security compatible. When setting up a communication, the caller provides the Zone Keeper security information in order for the caller to prove its identity. The callee supplies to the caller information confirming its identity. A proposal on how the communication is to be Set-up is sent from the caller to the callee, and if they agree to the proposal and their security is authenticated, the communication is started. For inter-zone, inter-domain, communications, the caller provides information as described above to its Zone Keeper. Then, the caller's Zone Keeper forwards the caller's request to the Zone Keeper of the security associated with the callee. Additionally, the caller's Zone Keeper also supplies the callee's Zone Keeper with its security identity so that the callee's Zone Keeper may authenticate that the request is from the caller's Zone Keeper. Then, the callee's Zone Keeper sends back an authorization to the Caller's Zone Keeper. This authorization includes the callee's Zone Keeper security identity so that the caller's Zone Keeper can authenticate that the authorization is from the callee's Zone Keeper. Then, as indicated above, the callee supplies to the caller information confirming its identity. A proposal on how the communication is to be Set-up is sent from the caller to the callee and if they agree to the proposal, and their security is authenticated, the communication is started.